[redacted]

SHEET 1 OF 5

FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use several sheets if necessary)

ATTY. DOCKET NO.
500.41092X00

SERIAL NO.
10/046,224

APPLICANT
M. NISHIOKA, et al

FILING DATE
January 16, 2002

GROUP
2136

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	ABSTRACT YES	ABSTRACT NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

		R. L. Rivest, et al "A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, vol. 21, No. 2. pp. 120-126, 1978.
		V. S. Miller, Use of elliptic curves in Cryptography, Proc. of Crypto '85, LNCS218, Springer-Verlag, pp. 417-426, 1985.
		N. Koblitz, Elliptic Curve Crytosystems, Math. Comp. 48, 177, pp. 203-209, 1987.

EXAMINER

DATE CONSIDERED 1/31/2006

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

SHEET 2 OF 5

FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** (Use several sheets if necessary)	ATTY. DOCKET NO. 500.41092X00	SERIAL NO. 10/046,224
	APPLICANT M. NISHIOKA, et al	
	FILING DATE January 16, 2002	GROUP 2136

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	ABSTRACT YES	ABSTRACT NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

DCC		M. O. Rabin, Digital Signatures and Public-key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCSTRANSMISSION-212, 1979.
DCC		T. El Gamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE, Trans. on Information Theory, IT-31, 4, pp. 469-472, 1985.
DCC		S. Goldwasser, et al Probabilistic Encryption, JCSS, 28, 2, pp. 270-299, 1984.

EXAMINER	DATE CONSIDERED 1/31/2006

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

SHEET 3 OF 5

FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** (Use several sheets if necessary)	ATTY. DOCKET NO. 500.41092X00	SERIAL NO. 10/046,224
	APPLICANT M. NISHIOKA, et al	
	FILING DATE January 16, 2002	GROUP 2136

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

							ABSTRACT	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

DGL		M. Blum et al, An Efficient Probabilistic Public-key Encryption Scheme which hides all Partial Information, Proc. of Crypto '84, LNCS196, Springer-Verlag, pp. 289-299, 1985.
DGL		S. Goldwasser, et al, Lecture Notes on Cryptography, http:/www-cse, ucsd.edu/users/mihir/1997.
DGL		T. Okamoto, et al, A new Public-key Cryptosystem as Secure as Factoring, Proc. of Eurocrypt '98, LNCS1403, Springer Verlag, pp. 308-318, 1998.

EXAMINER

DATE CONSIDERED 1/31/2006

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

SHEET 4 OF 5

FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** (Use several sheets if necessary)	ATTY. DOCKET NO. 500.41092X00	SERIAL NO. 10/046,224
	APPLICANT M. NISHIOKA, et al	
	FILING DATE January 16, 2002	GROUP 2136

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER							DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER							DATE	COUNTRY	CLASS	SUBCLASS	ABSTRACT	
													YES	NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

DCL		D. Dolve, et al Non-Malleable Cryptography, In 23rd Annual ACM Symposium on Theory of Computing, pp. 542-552, 1991.
DCL		M. Naor, et al Public-key Cryptosystems Provably Secure Against Chosen Ciphertext Attacks, Proc. of STOC, ACM Press, pp. 427-437, 1990.
DCL		M. Bellare, et al "Optimal Asymmetric Encryption How to Encrypt with RSA, Proc. of Eurocrypt '94, LNCS950, Springer Verlag, pp. 92-111, 1994.

EXAMINER	DATE CONSIDERED 1/31/2006

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

SHEET 5 OF 5

FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** (Use several sheets if necessary)	ATTY. DOCKET NO. 500.41092X00	SERIAL NO. 10/046,224
	APPLICANT M. NISHIOKA, et al	
	FILING DATE January 16, 2002	GROUP 2136

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	ABSTRACT YES	ABSTRACT NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

		R. Cramer et al, A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack, Proc. of Crypto '98, LNCS1462, Springer-Verlag, pp. 13-25, 1998.
		M. Bellare, et al Relations Among Notions of Security for Public-key Encryption Schemes, Proc. of Crypto '98, LNCS1462, Springer Verlag, pp. 26-45, 1998.

EXAMINER	DATE CONSIDERED 1/31/2006

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.